HISPOL 007.0

The United States House of Representatives Information Security Policy for the Information Security Compliance Program

Version:	**2.0**
Approved:	**January 2010**
Approval Authority:	**The United States House of Representatives Committee on House Administration**

Table of Contents

1 Introduction

Securing information systems is an effort built on the premise that information - in all forms and development phases - must be protected from unauthorized access, modification, disclosure, destruction, and denial of service, whether intentional or accidental. In order to protect information, the systems and applications that process, store, and transmit the information must be adequately protected. How one defines "adequately" depends on the sensitivity of the information, the degree of risk faced by the system/application, and the security controls and safeguards put in place to reduce that risk to an acceptable level.

The United States House of Representatives (House) Information Systems Security Program (ISSP) provides a strategy for ensuring adequate security is established and maintained throughout the system development life cycle (SDLC) for all House information systems. This policy complements the ISSP by presenting guidance on what constitutes adequate security in terms of minimum-security requirements, and describes how compliance with those requirements will be achieved and monitored.

Security requirements for House information systems differ based on the type of system. For the purposes of this policy, information systems are categorized as applications or network-aware devices. Applications may consist of one software system or a combination of hardware and software that support a function of House operations . Network-aware devices typically include, but are not limited to, wireless access points, servers, workstations, modems, printers, and multi-function devices that are capable of connecting to the House network. Throughout the remainder of this policy, a network-aware device is referred to as a "device" or "devices". Security requirements for the House network are established and maintained by the Information Systems Security Office (INFOSEC) in accordance with the ISSP.

1.1 Scope

This document has relevance to all House Offices and provides policy governing security and compliance requirements applicable to all information systems.

2 Policy Guidelines

The following policy guidelines address security requirements for House information systems:

1) House applications and devices shall be protected commensurate with the risk and magnitude of harm resulting from the loss, misuse, unauthorized access to, modification or destruction of information processed, stored, or transmitted.
2) Financial applications; i.e., systems of record that are significant to the financial reporting of the House, that are developed and implemented by the Chief Administrative Officer (CAO), the House network, and other applications as

requested (hereafter referred to as "affected applications") shall undergo certification to ensure appropriate security controls and safeguards have been implemented and are functioning.

3) Certification of affected applications will be conducted at least every three years. Reviews of devices will be conducted at least once every two years. These reviews may be conducted more frequently when a significant change occurs or at the discretion of INFOSEC.

4) Security requirements and controls for affected applications shall be identified and documented in a System Security Plan (SSP). SSPs shall be reviewed annually, updated as required, and include device-related security controls and documents as appropriate.

5) Security requirements and controls for each device shall be identified in the appropriate security standard(s).

3 Roles and Responsibilities

Individuals with key roles in the successful implementation of this policy, and their associated responsibilities, are described below.

3.1 Information Systems Security Office

The Information Systems Security Office (INFOSEC) provides oversight and guidance regarding the security of all House information systems. INFOSEC will:

1) Assess the adequacy, and coordinate the implementation, of security controls and safeguards.

2) Review and approve System Security Plans.

3) Conduct certification activities for affected systems prior to implementation and every three years thereafter; compliance reviews of devices every two years; and out-of-cycle reviews when a significant system change occurs or at the discretion of INFOSEC.

4) Provide security planning and risk management guidance and assistance to System Owners and Administrators.

5) Provide guidance in the appropriate security training for affected personnel in accordance with their responsibilities.

6) Establish, implement, and maintain appropriate security controls and safeguards on the House network.

3.2 Responsible House Offices and Personnel

House Offices are responsible for the procurement, development, integration, modification, operation, maintenance, and oversight of an information system. The responsible personnel, typically a designated System Owner, will:

1) Designate a primary point of contact for security-related issues.
2) Ensure a SSP is developed, reviewed annually, and maintained for affected applications.
3) Ensure the appropriate security standards are applied to applications and devices.
4) Ensure that information systems are deployed and operated according to agreed-upon security requirements.
5) Ensure users and support personnel receive appropriate security instruction.
6) Determine the sensitivity of information processed by, and ensure a risk assessment is conducted for, each affected application.
7) Implement appropriate controls for the generation, collection, processing, dissemination, storage, and disposal of information.

3.3 System Administrator

System Administrator roles are assigned to each device and are responsible for ensuring the appropriate operational security posture for each asset is maintained. The System Administrator will:

1) Serve as the INFOSEC primary point of contact for all matters related to security of devices.
2) Apply the appropriate security standard (s) for the device as part of the compliance review process.
3) Comply with applicable security policy requirements.
4) Work with INFOSEC to resolve security deficiencies and issues.

4 Certification

Certification is the process of defining and assessing security controls in an information system to determine the extent to which the controls are correctly implemented, operating as intended, and producing the required outcome with respect to meeting the protection requirements. Certification supports the risk management process by providing important information necessary to make credible, risk-based decisions on whether to place an application or device into operation or to continue their current operation.

The certification process for applications and devices is described below. They shall be certified prior to their initial implementation, and the process shall be repeated in the form of a compliance review whenever a significant system change occurs, or at least once every two years for devices, and once every three years for applications.

4.1 Applications

The certification of an affected application (CAO financial application, House network, other applications as requested) shall be based on:

- A review of the sensitivity of the application.
- A risk assessment identifying:
    - threats and vulnerabilities;
    - the potential impact and magnitude of harm to operations, assets, or individuals that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and the information system;, and
    - the effectiveness of current or proposed security controls.
- A review of the application's SSP.
- Compliance with the appropriate security standard(s).

Any security deficiencies found or issues identified shall be corrected or sufficiently addressed prior to receiving authority to operate from INFOSEC.

Applications not included in the defined "affected applications" shall be reviewed for compliance with the appropriate security standard(s) prior to implementation. Security deficiencies found in these applications will be addressed through the remediation process listed below.

4.2 Network-Aware Devices

Certification of devices shall be based on:

- Application and review of the appropriate security standard(s).
- Vulnerability assessment results.

High-risk devices (e.g., outward-facing servers), or those containing, processing, or transmitting highly sensitive data, may be subject to a more rigorous certification process and more frequent compliance reviews.

Any security deficiencies found or issues identified shall be corrected or sufficiently addressed as directed by INFOSEC.

4.3 Enterprise-Wide Security Assessments

In addition to assessing major and support applications and devices, INFOSEC conducts enterprise-wide security assessments of the House network. There are two classes of enterprise-wide security assessments:

- Quarterly vulnerability assessments.
- Immediate needs vulnerability assessments.

Approximately once every quarter, the House network is assessed to determine if devices contain network-based vulnerabilities. Enterprise-wide assessments are designed to identify common vulnerabilities that pose significant risk to the House network.

Immediate needs vulnerability assessments are conducted across the House network on an as-needed basis. These assessments are conducted when a software vendor releases a security bulletin concerning newly discovered, high-risk vulnerabilities that may exist on House devices. When technically possible, INFOSEC will devise a method to inspect all House devices for the existence of this specific vulnerability.

4.4 Security Remediation Process

Vulnerabilities identified during the review process of an application or device are documented and prioritized based on the risk each poses.

The level of risk each vulnerability poses is based on the sensitivity of the information processed and the type of access provided. In general, Internet-accessible devices and applications are given higher priority for remediation than those that are only accessible from the House internal network.

Once a vulnerability is identified, a corrective action is formulated and a timeframe established for its implementation. INFOSEC will coordinate with the Systems Owner or Administrator to ensure corrective action has taken place. Upon completion, INFOSEC will confirm the vulnerability has been mitigated.

For those vulnerabilities that have either no known corrective action or the implementation of a corrective action will seriously impair the functionality of the application, other compensating controls may be developed or a risk acceptance plan may be formulated.